



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|----------------------|------------------|
| 10/074,996 | 02/12/2002 | Chang-Ping Lee | SS-008 | 7160 |
| 22830 | 7590 | 06/29/2006 | EXAMINER | |
| CARR & FERRELL LLP 2200 GENG ROAD PALO ALTO, CA 94303 | | | REVAK, CHRISTOPHER A | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2131 | |

DATE MAILED: 06/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|---|-----------------------------------|--|
| Office Action Summary | Application No. 10/074,996 | Applicant(s) LEE ET AL. | |
| | Examiner Christopher A. Revak | Art Unit 2131 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 4/11/06.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed have been fully considered but they are not persuasive.

As per claims 1-10 and 24-30, it is argued by the applicant that England fails to disclose "determining....whether the file being accessed is secured" and "when the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application".

The examiner disagrees, the teachings of England disclose of determining whether the file is secured, see column 3, lines 14-17 & 35-42 and column 9, lines 30-39. It is further taught by England of activating a cipher module and loading the file through the cipher module into the application, see column 2, line 66 through column 3, line 13.

As per claims 11-19, the applicant argues that England fails to disclose "encrypting the file with the file key in a cipher module to produce an encrypted portion" and "preparing security information for the encrypted portion, the security information being encrypted and including the file key and access rules to control access to the encrypted portion".

The examiner respectfully disagrees, the teachings of England disclose of securing the file, see column 3, lines 14-17 & 35-42 and column 9, lines 30-39. It is

further taught by England of activating a cipher module and loading the file through the cipher module into the application, see column 2, line 66 through column 3, line 13. The security information is encrypted and including the file key and access rules to control access to the encrypted portion, see column 2, line 66 through column 3, line 13; column 12, lines 40-57; and column 14, lines 10-17.

As per claims 20-23, the applicant contends that England does not use secured files and fails to disclose “determining whether the file being accessed is secured”.

The examiner disagrees, the teachings of England disclose of determining whether the file being access is secured, see column 3, lines 14-17 & 35-42 and column 9, lines 30-39.

As per claims 31-39, it is argued by the applicant that England fails to teach “encrypting the file with the file key in a cipher module to produce an encrypted file” and “storing, in a storage space, a secured file including the encrypted file and a header”.

The examiner respectfully disagrees with the applicant’s assertion, England discloses of encrypting the file with the file key in a cipher module to produce an encrypted file, see column 2, line 66 through column 3, line 13 and column 9, lines 30-39. It is further taught by England of storing a secured file including the encrypted file and a header, see column 14, lines 10-17.

As per claims 40-50, the applicant argues that England fails to disclose "accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted version of the file."

The examiner disagrees with the applicant's assertion, England discloses accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted version of the file, see column 2, line 66 through column 3, line 13; column 12, lines 40-57; and column 14, lines 10-17.

2. The rejections under 35 USC 101 and 35 USC 112 2nd paragraph have been withdrawn.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-50 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al, U.S. Patent 6,775,779.

As per claims 1 and 24, it is disclosed by England et al of a method and a software product for securing a file, the method comprising launching an application when a request to access the file is received, determining, in an operating system supporting the application, whether the file being accessed is secured, when the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application, when the file is determined to be non-secured, loading the file into the application without activating the cipher module (col. 2, line 66 through col. 3, line 13 and col. 9, line 55 through col. 10, line 5).

As per claim 2, England et al teaches that the cipher module, once activated, operates within the operating system (col. 10, lines 28-36).

As per claim 3, England et al recites that the cipher module, once activated, operates transparently to a user requesting an access to the file (col. 10, lines 28-36).

As per claims 4 and 25, England et al teaches that the secured file includes a header and an encrypted portion, the header including or pointing to security information including a file key that, once obtained, can be used to decrypt the encrypted portion (col. 14, lines 18-35).

As per claims 5 and 26, England et al discloses of determining of whether the file being accessed is secured comprises determining if the file being accessed includes the header (col. 14, lines 18-35).

As per claim 6, England et al teaches that the header further includes a flag indicating that the file being accessed is secured, and wherein the determining of

whether the file being accessed is secured comprises determining if the file has the flag (col. 2, line 66 through col. 3 and col. 14, lines 18-35).

As per claims 7 and 27, the teachings of England et al recite wherein the loading of the file through the cipher module into the application comprises retrieving the file key, decrypting the encrypted portion with the file key in the cipher module, and sending the file in clear mode to the application (col. 14, lines 18-35).

As per claims 8 and 28, it is disclosed by England et al that the security information including the file key is encrypted with a user key, and wherein the retrieving of the file key comprises obtaining a user key associated with a user requesting an access to the file, and decrypting the encrypted security information with the user key to retrieve the file key (col. 14, lines 18-35).

As per claims 9 and 29, England et al discloses that the security information further includes access rules controlling how and who the secured file can be accessed (col. 6, lines 33-45).

As per claims 10 and 30, the teachings of England et al recite wherein the loading of the file through the cipher module into the application only happens when access privilege of the user is within permissions granted by the access rules (col. 6, lines 33-45).

As per claim 11, England et al teaches of a method for securing a file, the method comprising maintaining a file key in a temporary memory space, encrypting the file with the file key in a cipher module to produce an encrypted portion, preparing security information for the encrypted portion, the security information being encrypted

and including the file key and access rules to control access to the encrypted portion, and attaching the encrypted security information to the encrypted portion (col. 2, line 66 through col. 3, line 13 and col. 9, line 55 through col. 10, line 5).

As per claim 12, England et al teaches of deleting the file key from the temporary memory space when the attaching of the encrypted security information to the encrypted portion is complete (col. 10, lines 28-56).

As per claim 13, England et al discloses that wherein the encrypting of the file with the file key, the preparing of the security information, and the attaching of the encrypted security information happen whenever the file is caused to be stored in a storage space (col. 14, lines 18-35).

As per claim 14, it is disclosed by England et al wherein the encrypting of the file with the file key, the preparing of the security information, and the attaching of the encrypted security information happen upon receiving an instruction from an application or an operating system supporting the application (col. 10, lines 28-36 and col. 14, lines 18-35).

As per claim 15, England et al teaches wherein the application is provided in Microsoft Office and the operating system is Microsoft Windows (col. 5, lines 15-20).

As per claim 16, it is disclosed by England et al that the instruction is one of (i) Save, (ii) Close and (iii) Exit, all provided in the application (col. 10, lines 28-36).

As per claim 17, England et al teaches that the instruction is generated from an automatic operation of saving the file being opened into the storage space, the

automatic operation is either triggered by the application itself or the operating system (col. 10, lines 28-56).

As per claim 18, England et al recites of encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group of users (col. 14, lines 18-35).

As per claim 19, England et al teaches wherein the access rules in the security information comprises user information identifying who can assess the encrypted portion and how the encrypted portion can be accessed (col. 6, lines 33-45).

As per claim 20, England et al discloses a method for providing access control to a file, the method comprising launching an application under an operating system when a request to access the file is received, forwarding the request to a file system manager in the operating system, activating a document securing module by the file system manager to determine whether the file being accessed is secured, activating a cipher module when the file is determined to be secured, and loading the file through the cipher module into the application (col. 2, line 66 through col. 3, line 13 and col. 9, line 55 through col. 10, line 5).

As per claim 21, England et al recites of retrieving security information from the file when the file is determined to be secured, the security information including a file key and access rules, and obtaining an access privilege of a user requesting to access the file (col. 6, lines 33-45).

As per claim 22, the teachings of England et al recite wherein the activating of the cipher module proceeds successfully when the access privilege is within permissions granted by the access rules (col. 6, lines 33-45).

As per claim 23, it is disclosed by England et al wherein the activating of the cipher module comprises decrypting an encrypted portion of the secured file with the file key (col. 2, line 66 through col. 3, line 13 and col. 14, lines 18-35).

As per claim 31, England et al teaches of a software product including computer instructions for securing a file, the instructions, when executed by a processor, cause the processor to perform operations of maintaining a file key in a temporary memory space, encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and the cipher module operates transparently as far as a user executing the application is concerned, and storing, in a storage space, a secured file including the encrypted file and a header, wherein the header includes or points to security information including the file key (col. 2, line 66 through col. 3, line 13 and col. 9, line 55 through col. 10, line 5).

As per claim 32, England et al discloses of deleting the file key from the temporary memory space when the application is caused to close the file (col. 10, lines 28-56).

As per claim 33, England et al teaches wherein the encrypting of the file with the file key happens whenever the file is caused to be stored in the storage space (col. 10, lines 28-56).

As per claim 34, England et al recites wherein the encrypting of the file with the file key happens upon receiving an instruction from the application or an operating system supporting the application (col. 10, lines 28-56 and col. 14, lines 18-35).

As per claim 35, England et al teaches wherein the instruction is one of (i) Save, (ii) Close and (iii) Exit, all provided in the application (col. 10, lines 28-36).

As per claim 36, England et al discloses wherein the instruction is generated from an automatic operation of saving the file being opened into the storage space, the automatic operation is either triggered by the application itself or the operating system (col. 10, lines 28-56).

As per claim 37, England et al discloses wherein the security information further includes access rules of how and who the secured file can be accessed (col. 6, lines 33-45).

As per claim 38, it is taught by England et al of encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group (col. 14, lines 18-35).

As per claim 39, England et al recites of attaching the header to the encrypted file, wherein the header includes the security information encrypted in addition to a flag indicating that the file is secured (col. 14, lines 18-35).

As per claim 40, England et al teaches of a computing device for securing a file, the computing device comprising an application, when executed, accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted

version of the file, a cipher module activating upon determining that the file being accessed is secured, wherein the security information is encrypted and can be decrypted with a user key when authenticated; and wherein the file key can be retrieved to decrypt the encrypted portion only after the access rules have successfully measured against access privilege of the user (col. 2, line 66 through col. 3, line 13; col. 9, line 55 through col. 10, line 5; and col. 6, lines 33-45).

As per claim 41, England et al discloses of an operating system supporting operations of the application, and wherein the cipher module is embedded in the operating system (col. 10, lines 28-36).

As per claim 42, England et al discloses wherein the cipher module operates in a path through which the file is caused to pass when accessed by the application (col. 10, lines 28-56).

As per claim 43, England et al teaches that the computing device further including a memory space and a storage space, and wherein the file key is temporarily kept in the memory space when the file is successfully loaded into the application (col. 10, lines 28-56).

As per claim 44, it is disclosed by England et al wherein the file key is deleted from the memory space as soon as the file is wrote back to the storage space (col. 10, lines 28-56).

As per claim 45, England et al teaches wherein the user key becomes authenticated only when the user is authenticated by an authentication process to verify

who the user claims to be (col. 11, line 55 through col. 12, line 5 and col. 13, lines 60-66).

As per claim 46, England et al discloses wherein the computing device is coupled to another computing device over a data network, the user key becomes authenticated only after the user is successfully logged from the computing device into the another computing device (col. 11, line 55 through col. 12, line 5 and col. 13, lines 60-66)

As per claim 47, England et al teaches wherein the computing device is provided with means for capturing biometric data of the user, the user key becomes authenticated only after the biometric data is successfully verified to support who the user claims to be (col. 11, line 55 through col. 12, line 5 and col. 13, lines 60-66).

As per claim 48, it is taught by England et al wherein the user key becomes authenticated after the computing device receives credential information from the user (col. 11, line 55 through col. 12, line 5 and col. 13, lines 60-66).

As per claim 49, England et al discloses wherein the credential information includes one of a password entered by the user, biometric information of the user, personalized information about the user (col. 11, line 55 through col. 12, line 5 and col. 13, lines 60-66).

As per claim 50, England et al recites wherein the biometric information is captured from a device coupled to the computing device (col. 11, line 55 through col. 12, line 5 and col. 13, lines 60-66).

Conclusion


5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CR 
June 26, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

 6/26/06